6712-01

This document is scheduled to be published in the Federal Register on 03/11/2022 and available online at **federalregister.gov/d/2022-05121**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

[PS Docket No. 22-90, FCC 22-18; FRS 75229]

Secure Internet Routing

AGENCY: Federal Communications Commission.

ACTION: Request for comments.

SUMMARY: In this document, the Federal Communications Commission (FCC or the Commission) seeks comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9-1-1 calls, and how best to address them.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**; and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by PS Docket No. 22-90, by any of the following methods:

- *Electronic Filers*: Comments may be filed electronically by accessing ECFS at https://www.fcc.gov/ecfs.
- *Paper Filers*: Paper filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.
- *People with Disabilities*: To request materials in accessible formats for people with

disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

For detailed instructions for submitting comments and additional information on this proceeding, see the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT: For additional information on this proceeding, contact James Wiley of the Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at james.wiley@fcc.gov or (202) 418-1678 or Minsoo Kim of the Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at minsoo.kim@fcc.gov or (202) 418-1739.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Inquiry, FCC 22-18, released February 28, 2022. The full text of this document is available at https://www.fcc.gov/document/fcc-launches-inquiry-internet-routing-vulnerabilities.

Ex Parte Rules. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. Although the rules do not generally require *ex parte* presentations to be treated as "permit but disclose" in Notice of Inquiry proceedings, the Commission exercises its discretion in this instance, and finds that the public interest is served by making *ex parte* presentations available to the public, in order to encourage a robust record. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data

presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b), 47 CFR § 1.1206(b). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

Confidentiality. The Commission recognizes that some comments could contain information that the submitter believes should not be made available to the general public because of commercial or national security reasons. Parties may request that such information be kept confidential, identifying the specific information sought to be kept confidential, providing the reasons for the request, and otherwise following the procedures set forth in section 0.459 of the Commission's rules. If a party requests confidential treatment of a comment, it must file an original and one copy of the confidential version of the comment on paper, following the procedures below, and a public version of the filing that omits only the confidential information and is otherwise identical to the confidential version, using either the electronic filing or the filing-by-paper procedures below

Comment Filing Procedures. Interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS) or by paper. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing. Paper filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
    - Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.
    - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, D.C. 20554.

Availability of Documents. Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. These documents will also be available for public inspection during regular business hours in the FCC Reference Information Center, when FCC Headquarters reopen to the public.

People with Disabilities. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

Synopsis

1. The Commission plays an important role in protecting the security of America's communications networks and critical infrastructure. The Commission, in tandem with its federal partners, has urged the communications sector to defend against cyber threats, while also taking measures to reinforce our Nation's readiness and to strengthen the cybersecurity of vital communications services and infrastructure, especially in light of Russia's escalating actions inside of Ukraine. Today, the Commission builds on those efforts. With this *Notice of Inquiry* (*Notice*), the Commission seeks comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9-1-1 calls, and how best to address them.

2. BGP is the routing protocol used to exchange reachability information amongst independently managed networks on the Internet. These independently managed networks (also termed "domains") loosely map to one or more "Autonomous Systems" (so termed because the administration of the network is the sole responsibility of a single, independent entity). BGP's initial design, which remains widely deployed today, does not include security features to ensure trust in the information that it is used to exchange. BGP was designed at a time when the number of independently managed networks on the Internet was low and the trust among them was high. As a result, a bad network actor may deliberately falsify BGP reachability information to redirect traffic to itself or through a specific third-party network, and prevent that traffic from reaching its intended recipient. When a bad actor directs traffic to be dropped in this way, it is commonly referred to as a "blackhole." These "BGP hijacks" expose U.S. citizens' personally identifiable information, enable theft, extortion, and state-level

espionage, and disrupt otherwise-secure transactions. The Commission uses the term "BGP hijacking" to refer to any deliberate injection of routing information away from the optimal (or most secure) route, including both false route origination and path interception attacks.

3. Congress created the Commission, among other reasons, "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications." To obtain "maximum effectiveness from the use of radio and wire communications in connection with the safety of life and property," the Communications Act of 1934, as amended, directs the Commission to "investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination" of such systems."

4. The Commission has taken targeted steps to protect the nation's communications infrastructure from potential security threats. Most recently, the Commission encouraged communications companies to review cybersecurity practices to defend against threats to critical infrastructure, sought comment on how the Commission can leverage its equipment authorization program to encourage device manufacturers to consider cybersecurity standards and guidelines, and acted in the public interest to deny and revoke the section 214 authority of certain carriers to provide telecommunications service in the United States.

5. Independently managed networks are essential to the daily functioning of critical infrastructure such as transportation, gas and electric power, water, and financial markets. These networks can be vulnerable to attack if they deploy a version of BGP at their borders that cannot verify the integrity or authenticity of routing information. These vulnerabilities have two main causes: (1) validating a route's origin; and (2) securing and validating the correct BGP path to a given destination. BGP's vulnerabilities allow a network operator to accidentally or maliciously misconfigure its BGP routers to falsely advertise that its network contains the intended destination for certain Internet traffic, or is on the path to that destination. By

advertising incorrect routing information, a bad actor could spread incorrect information to other networks and cause traffic intended for the advertised destination to be misrouted to, or through, the bad actor's network. Causing Internet traffic to depart from its most efficient path is termed "BGP hijacking." Although BGP hijacking can occur anywhere on the global Internet, the Commission has an interest in minimizing or eliminating opportunities for it within its jurisdiction because it can potentially harm U.S. citizens, commerce, and public safety operations.

6. Russian network operators have been suspected of exploiting BGP's vulnerability to hijacking, including instances in which traffic has been redirected through Russia without explanation. In late 2017, for example, traffic sent to and from Google, Facebook, Apple and Microsoft was briefly routed through an Internet service provider in Russia. That same year, traffic from a number of financial institutions, including MasterCard, Visa, and others was also routed through a Russian government-controlled telecommunications company under "unexplained" circumstances.

7. Over the past two decades, Internet stakeholders have developed new standards, specifications, and best practice recommendations intended to address the security risk that BGP poses. The Internet Engineering Task Force (IETF), the principal authority responsible for Internet standards, has finalized several standards to reduce BGP vulnerabilities, including BGPsec, an extension to BGP that provides security for the path through which reachability information passes. The National Institute of Standards and Technology (NIST) has released a practice guide proposing a method of validating routes' origins and recommendations for resilient exchange between independently managed networks. In 2017, the Internet Society launched Mutually Agreed Norms for Routing Security (MANRS), an organizational initiative with membership including over 700 network operators, Internet Service Providers, and enterprises, which aims to reduce or prevent route hijacking and denial

of service attacks by requiring network operators to implement available tools and applicable IETF Best Common Practice standards. MANRS focuses on improving routing security by filtering routing advertisements to include only those likely to be relevant to the customer BGP router; enabling source IP address validation for customer networks; coordinating and sharing contact information for network operations center contacts through regional Internet registries, and enabling routing information to be validated on a global scale. MANRS offers a tool called "MANRS Observatory" that aggregates data from trusted sources into a dashboard to help network operators improve the security of their networks. Similarly, the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) has reported on best practices and recommendations to improve the security of BGP. The roman numerals following the name of federal advisory committee, "CSRIC," enumerate the successive years during which the Commission has chartered CSRIC to provide recommendations on selected topics. CSRIC III recommended that network operators ensure that BGP routers' Internet routing registries are accurate, complete, and up-to-date, and that network operators use a standards-based approach for providing cryptographically secure registries of Internet resources and routing authorizations, a Resource Public Key Infrastructure (RPKI). In this connection, the FCC sought comment on the implementation and effectiveness of the CSRIC III recommendations and/or alternatives that stakeholders have developed since the time of the CSRIC's original work to address these challenges. CSRIC VI recommended that network operators support MANRS and IETF Best Common Practice standards. Notwithstanding this work, available information suggests that the voluntary adoption and deployment of such measures has been such that many of the independently managed networks that comprise the Internet remain vulnerable because they have not taken advantage of these measures.

8. *Scope of Inquiry.* In this *Notice*, the Commission seeks comment on any steps that the Commission should consider taking to help protect and strengthen the nation's

communications network and other critical infrastructure from vulnerabilities posed by BGP, and how the Commission can best facilitate the implementation of industry standards and best practices to mitigate the potential harms posed by these vulnerabilities. In order to better understand the BGP ecosystem, the Commission seeks comment on the extent to which Internet Service Providers, public Internet Exchange Providers, and providers of interconnected VoIP service have deployed BGP routers in their networks. Do content delivery networks, and providers of cloud services operate BGP routers in their networks as well? What other types of entities operate BGP routers? The Commission recognizes that there are entities that do not operate BGP routers, but that are otherwise well positioned to support the development and implementation of BGP security practices. For example, there are several regional, national, and local Internet registries that manage the allocation and registration of Internet number resources, and support RPKIs. As an example, one such regional Internet registry, the American Registry for Internet Numbers (ARIN) supports the roles of a digital certificate authority and acts as a repository for routing information and as a validator of RPKI data. Additionally, the Internet Corporation for Assigned Names and Numbers (ICANN), through its affiliate, Internet Assigned Numbers Authority (IANA), has responsibility for coordinating the Internet's unique identifiers. The Commission seeks comment on what role these and other entities, including vendors of BGP routers or other networking equipment, have in supporting the development and implementation of BGP security practices. What threats to Internet routing should the Commission consider within the scope of this inquiry in addition to BGP hijacking? For example, to what extent could BGP security measures prevent pervasive monitoring?

9. *Measuring BGP Security.* The Commission seeks comment on whether industry has defined metrics for identifying BGP routing security incidents and for quantifying their scope and impact. To what extent are available tools, such as NIST's RPKI Monitor, Automatic and Real-Time dEtection and Mitigation System (ARTEMIS), BGPstream, BGPMon, Kentik, and

Traceroute, able to rapidly and accurately detect BGP hijacks or router misconfigurations? To what extent do these tools distinguish malicious routing changes from accidental ones? Do artificial intelligence and machine learning tools promise advancements in this area?

10. *Deployment of BGP Security Measures.* The Commission seeks comment on the security measures that have been developed and deployed by industry to secure BGP. In addition to the measures recommended by CSRIC III and VI (RPKI, MANRS, and applicable IETF Best Common Practice standards), BGPsec, and the NIST practice guide, what other standards, specifications, or best practices have been developed to address potential attacks that exploit BGP vulnerabilities? The Commission seeks comment on the extent to which network operators have implemented any of the available BGP security measures developed by industry. How effective are these measures in practice? The Commission seeks comment on how to assess, measure, demonstrate, or increase the effectiveness of these security measures. To the extent that network operators have not implemented security measures, the Commission seeks comment on why such measures have not been implemented. To the extent that network operators have implemented security measures, how effective have they been at mitigating the vulnerability? What obstacles have prevented them from doing so?

11. The Commission seeks comment on the extent to which RPKI, as implemented by other regional Internet registries, effectively prevents BGP hijacking. To what extent do network operators take advantage of the RPKI services that regional Internet registries offer by implementing RPKI in their networks? To what extent, if any, do network operators' service level agreements affect the ability of network operators to drop traffic that RPKI deems invalid? How do regional Internet registries maintain the certificate authority for the RPKIs in a way that mitigates the risk of a single point of failure vulnerable to distributed denial of service attacks? How do regional Internet registries prevent conflicts among distributed RPKI trust anchors?

12. The Commission seeks comment on whether and to what extent network operators anticipate integrating BGPsec-capable routers into their networks. The specification for the BGPsec extension to BGP became available in 2017, but it appears that BGPsec has not been widely deployed despite BGP's known vulnerabilities. Why have network operators not taken more aggressive steps to adopt BGPsec? What particular obstacles or concerns about BGPsec have slowed their adoption? To what extent does the introduction of BGPsec routers potentially introduce compatibility issues among managed networks or introduce delays?

13. For network operators that currently participate in MANRS and comply with its requirements, including support for IETF Best Common Practice standards, the Commission seeks comment on the efficacy of such measures for preventing BGP hijacking. To what extent do the network operators that participate in MANRS support both its required and recommended routing security actions, as well as applicable IETF Best Common Practice standards on which those actions are based? To what extent do network operators participate in MANRS' various programs, including its equipment vendor program, launched in 2021, which aims to enable routing security features on network equipment and provide support and training guidance to use them, or take advantage of the MANRS Observatory.

14. *Commission's Role.* Ensuring continued U.S. leadership requires that the Commission explores opportunities to spur trustworthy innovation for more secure communications and critical infrastructure. The Commission has sought to promote the security of U.S. networks and network equipment both by drawing attention to available resources and through exercise of its regulatory authority. Other federal agencies are engaged in cybersecurity and specifically BGP security, including NIST, the Department of Homeland Security, and the National Telecommunications and Information Administration. The Commission seeks comment on steps the Commission, in coordination with other federal agencies, could take to prevent BGP hijacking or otherwise promote secure Internet routing.

The Commission seeks comment on whether the Commission has a role in helping U.S. network operators deploy BGP security measures. If so, how can the Commission be most helpful? The Commission seeks comment on its authority to promote the security of Internet routing through regulation, including as it may apply to wireless and wireline Internet Service Providers, Internet Exchange Providers, interconnected VoIP providers, operators of content delivery networks, cloud service providers, and other enterprise and organizational stakeholders. The Commission seeks comment on whether regulatory clarity could help network operators prioritize investments in the security of their networks.

15. The Commission seeks comment on the extent to which other nations' telecommunications regulators and multistakeholder organizations have issued rules, guidance, or otherwise encouraged network operators, network security organizations, and equipment vendors to implement BGP security measures and on any lessons learned from those endeavors. The Commission seeks comment on the extent to which the effectiveness of BGP security measures may be related to international participation and coordination.

16. *Costs and Benefits.* The Commission seek comments on the one-time and ongoing costs of implementing the BGP security measures discussed herein. What capital and operational expenditures attend their implementation? Does the availability of a protocol for RPKI keep implementation costs low? Would network operators need to replace existing routers to support the BGPsec extension? Could support be enabled through a software upgrade, particularly for routers that are not considered to be "end-of-life"? To what extent can network operators support MANRS' required and recommended actions by updating their policies and practices, and without equipment replacement or software updates? What costs would consumer likely experience from BGP security implementations, such as higher service costs or speed reductions?

17. The Commission seeks comment on whether the Commission should encourage industry to prioritize the deployment of BGP security measures within the networks on which critical infrastructure and emergency services rely, as a means of helping industry to control costs otherwise associated with a network-wide deployment. Would this or another phased or gradual implementation of BGP security measures be effective and help network operators to plan for and control implementation costs?

18. The Commission also seeks comment on the national security, economic, and public safety benefits of more secure Internet routing, both within the U.S. and globally. What entities are particularly affected by threats to BGP security? To what extent would the security measures discussed herein be effective in mitigating BGP hijacking? What is the potential impact of mitigating BGP hijacking on U.S. national security and the U.S. economy? Have stakeholders attempted to quantify the benefits that secure Internet routing could convey by protecting critical infrastructure, sensitive communications, and personally identifiable information? Have stakeholders attempted to quantify the benefits of secure Internet routing in terms of the potential loss of Intellectual Property, communications delays, or disruptions that BGP's unmitigated vulnerability represents? Have stakeholders attempted to measure or quantify the extent to which BGP hijacking poses a threat to life and property by disrupting 9-1-1 calls carried by providers of interconnected VoIP service? What other benefits could potentially accrue from this inquiry?

19. *Digital Equity and Inclusion.* Finally, the Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. Section 1 of the Communications Act of 1934

as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex." The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. Specifically, the Commission seeks comment on how its proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

20. Authority for this Notice of Inquiry may be found in sections 1, 4(i)-(j), 4(n), 7, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i)-(j), 154(n), 157 and Section 1.430 of the Commission's rules, 47 CFR 1.430.

Federal Communications Commission.

Marlene H. Dortch,

Secretary,

Office of the Secretary.

[FR Doc. 2022-05121 Filed: 3/10/2022 8:45 am; Publication Date: 3/11/2022]